
# User Manual

## Get Console Private Server

Version: 1.5.1

Date: 5 December 2013

## CONTENTS

## REVISION HISTORY

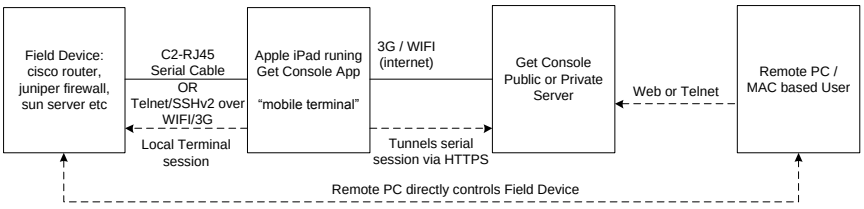
| Revision | Date | Description | Author |
|---|---|---|---|
| 1.04 | 5 May 2011 | First Release | SH / RP |
| 1.20 | 30 August 2011 | Second Release for Private Server v1.2 | SH / RP |
| 1.5.1 | 4 December 2013 | Update for Private Server version 1.5 | SH / EH |

## WHAT IS GET CONSOLE PRIVATE SERVER?

There are 2 Components to the Get Console solution

1) The Get Console App which runs on Apple iPads and iPhones
2) The Get Console Server which can be either the Public or Private version

The below drawing summarizes the components of Get Console




## GET CONSOLE APP

The Get Console app provides iPads and iPhones with terminal connectivity via **Serial**, **Telnet** or **SSH(v2)** to IT equipment (for example, a Cisco router or a Linux Server). This allows a field engineer to configure such IT equipment in the field using the apps intuitive terminal window. The app can then optionally act as a

terminal server to share its serial/Telnet/SSH sessions with remote users via a Get Console Server (Public or Private).

The app is designed primarily to be a mobile terminal – it enables field engineers connect to and configure network devices and servers via these devices' serial console ports (or SSH/Telnet server), and then, if required, use the Apple 3G or WIFI connection to share the terminal window.

## GET CONSOLE SERVER

There are 2 versions of the Get Console Server

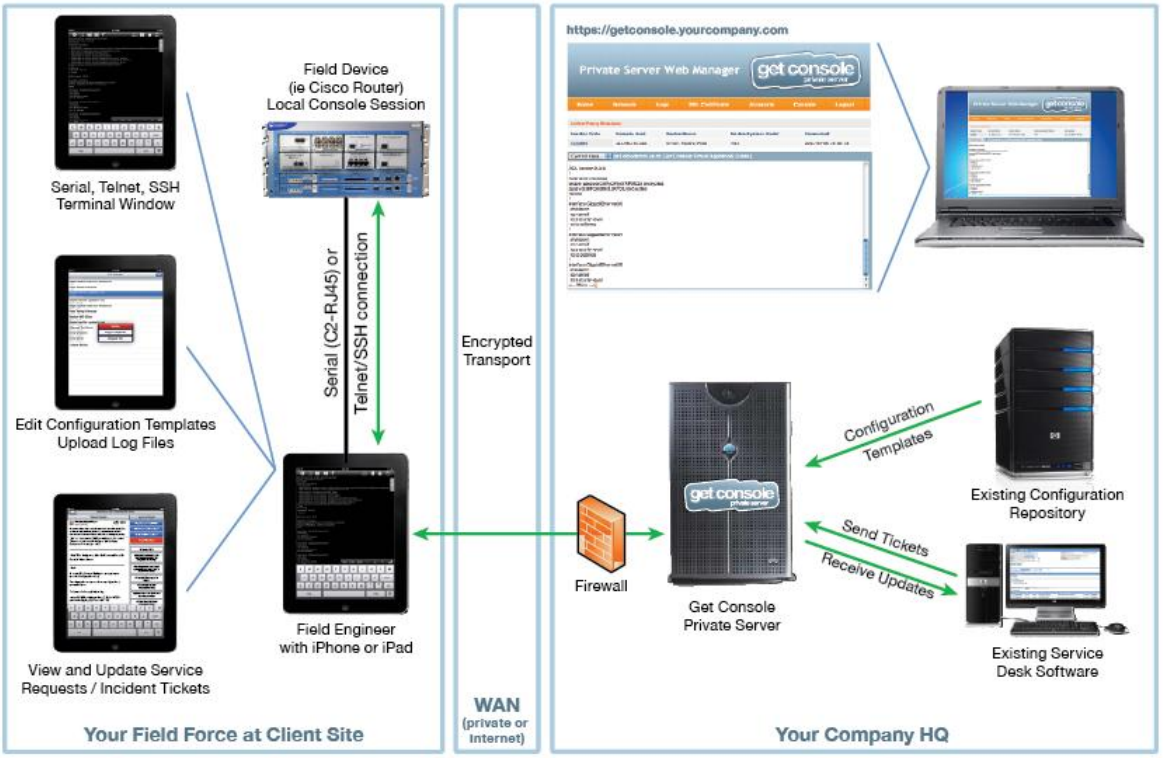
1) The publicly available Get Console Servers hosted at the website www.get-console.com
2) The private version, which is hosted on a customers own network, and secured by their own network security policy (the subject of this user manual).

Both versions of the Get Console Server acts as a connection broker and proxy between the Apple iPad/iPhone terminal session and the remote users sitting at PCs, allowing the remote PC user to control the terminal session connected to the Apple iPad/iPhone.

Public versions of the Server are hosted in US, UK and New Zealand. These can be used at no charge by any registered purchasers of the Get Console App to allow any remote PC to access the terminal session via the public website www.get-console.com. The performance of the end to end terminal varies greatly on the current load of the server and the latency of both the Apple device and the Remote PC users from the selected public server.

The Get Console Private Server extends the functionality of the Get Console solution by allowing end users or corporations to deploy their own privately hosted version of the Get Console public server component. This has the following benefits:

- Increased Security, as the Private Server and Remote PC user are located behind the corporate firewall, so no potentially sensitive field device configurations or data is transmitted through or stored on the public Get Console servers. In addition, the Private Server can install a valid corporate SSL certificate to allow the Apple device to Private Server connection to use SSL encryption.
- Increased Performance, as the latency between the Remote PC user and the Private Server is greatly reduced meaning the end to end performance of the remote control terminal session is fast and smooth
- Increased Flexibility, as the Remote PC user can use either the Private Servers built in Web Terminal, or any Telnet client of their choosing (such as SecureCRT, or puTTy)
- Increased Ease of Use, as the Private Server displays all currently available sessions and the name of the mobile terminal associated (generally the field engineers name). The field engineer does not need to pass the session code number to the remote PC user, as the remote PC user can see all the sessions and quickly identify the session he wants to connect to.
- Upload and Manage corporate configuration templates for field devices and download them to the iPad/iPhone in the field
- Keep log files of all field terminal sessions and upload them automatically for audit trail and troubleshooting


Field Device
(ie Cisco Router)
Local Console Session
Serial, Telnet, SSH
Terminal Window
Serial (C2-RJ45) or
Telnet/SSH connection
Edit Configuration Templates
Upload Log Files
Encrypted
Transport
View and Update Service
Requests / Incident Tickets
Field Engineer
with iPhone or iPad
Your Field Force at Client Site
WAN
(private or
Internet)
https://getconsole.yourcompany.com
Private Server Web Manager
get console
Configuration
Templates
Existing Configuration
Repository
Send Tickets
Receive Updates
Firewall
Get Console
Private Server
Existing Service
Desk Software
Your Company HQ

## OBTAINING THE PRIVATE SERVER SOFTWARE

The Get Console Private Server software is a free download available from the www.get-console.com/private-server website. The file is packaged as either an OVF (Open Virtualization Format) package, or a VMWare vmx/vmdk package. While the download is free, the Server will not work with Apple iOS devices until it is licensed (see licensing section below).

Get Console offers support for VMWare Server 2.0 or vSphere 4.0 and above installation of the vmx/vmdk package. The OVF format package is supplied for other non-VMWare virtualization hypervisors, however it has not been tested on other hypervisors.

If you are running VMWare we recommend downloading the VMX/VMDK zip file and install as per the instructions in the later sections.

### VIRTUAL APPLIANCE REQUIREMENTS

The Get Console Private Server Appliance has the following minimum specification:

Operating System: Centos 5.5 **64 bit**
CPU: 1 Processor
Memory: 1 GB
HDD: 5 GB

VMWare Hardware Version Support Required: **version 7**

*As the Get Console Private Server is a 64 bit "Guest OS" appliance. It will only run on a 32 bit host operating system if the underlying CPU of the physical host machine is 64 bit capable*. See the following table from vmware.com to understand compatibility.

| | **Host OS** | **32-Bit Guest OS** | **64-bit Guest OS (ie Get Console)** |
|---|---|---|---|
| **32-Bit CPU** | 32-Bit Host OS | Supported | Unsupported |
| | 64-Bit Host OS | Unsupported | Unsupported |
| **64-Bit CPU** | 32-Bit Host OS | Supported | Supported |
| | 64-Bit Host OS | Supported | Supported |

Private Server (v1.3 and later) can also integrate with an existing corporate trouble ticket system. If this feature is enabled, the Private Server will require its own email account on the corporate mail server, and rights on this server to send mail via SMTP (port25) and be able to POP its mail account (port 110).

### FIREWALL PORT REQUIREMENTS

The following Table describes the ports used by the Private Server. These ports will need to be open to the Private Server from any intervening firewall.

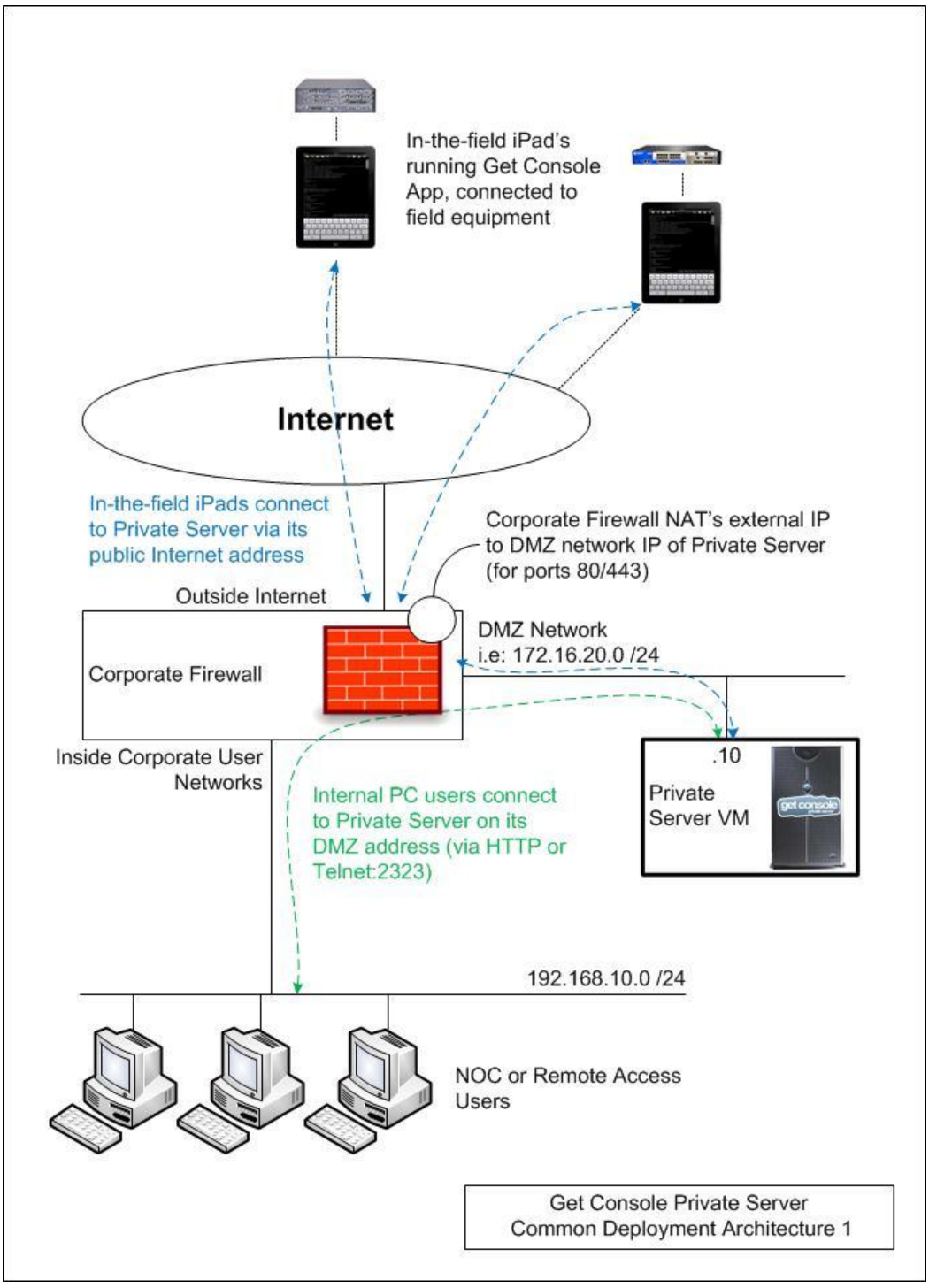
| **TCP Port** | **Description** | **Used For** |
|---|---|---|
| **80** | HTTP | From iPhone/iPad to Private Server tunnelling serial session to Private Server<br>From Remote PC user to Private Server for accessing the admin and web-terminal function |
| **443** | HTTPS | (Where SSL certificate has been installed, and the secure connection is selected in the iPad / |

| | | |
|---|---|---|
| | | iPhone app settings) From iPhone/iPad to Private Server tunnelling serial session to Private Server From Remote PC user to Private Server for accessing the admin and web-terminal function<br><br>This port is also used outbound from the Private Server to check the www.get-console.com website for software updates. |
| **2323** | Telnet | From NOC/Remote User PC to Private Server (if using third party telnet client (ie SecureCRT/Putty) |
| **25** | SMTP | (optiona) used between Private Server and user defined mail gateway – used for sending updates to troubletickets / service requests back to existing corporate ticket service desk software |
| **110** | POP | (optional) used from Private Server to download its troubletickets from its user provided mailbox on the Corporate email system |

In addition to the above TCP port requirements, a general requirement of Private Server licensing is the provision of Private server on a Static IP address. The IP address can be either public or private, however in order to successfully license Private Server it cannot dynamically change.

## COMMON DEPLOYMENT ARCHITECTURE

The below drawing describes the most common high level network design for deploying Private Server.




While not the only method, this design allows the Private Server to be securely placed where remote internet connected iPads and iPhones can reach it, while also allowing secure access from internal users.

Other alternatives include forcing internet connected iPads and iPhones to use the iPad/iPhones built in Cisco VPN client to build a IPSEC VPN tunnel to the Corporate Firewall (VPN Concentrator) and then launch the Get Console session sharing connection to the Private Server. This alternative alleviates the need for NAT, and also means Private Servers hosted behind dynamic public IP addresses can be used via a static internal private IP address.

# INSTALLING VMWARE APPLIANCE

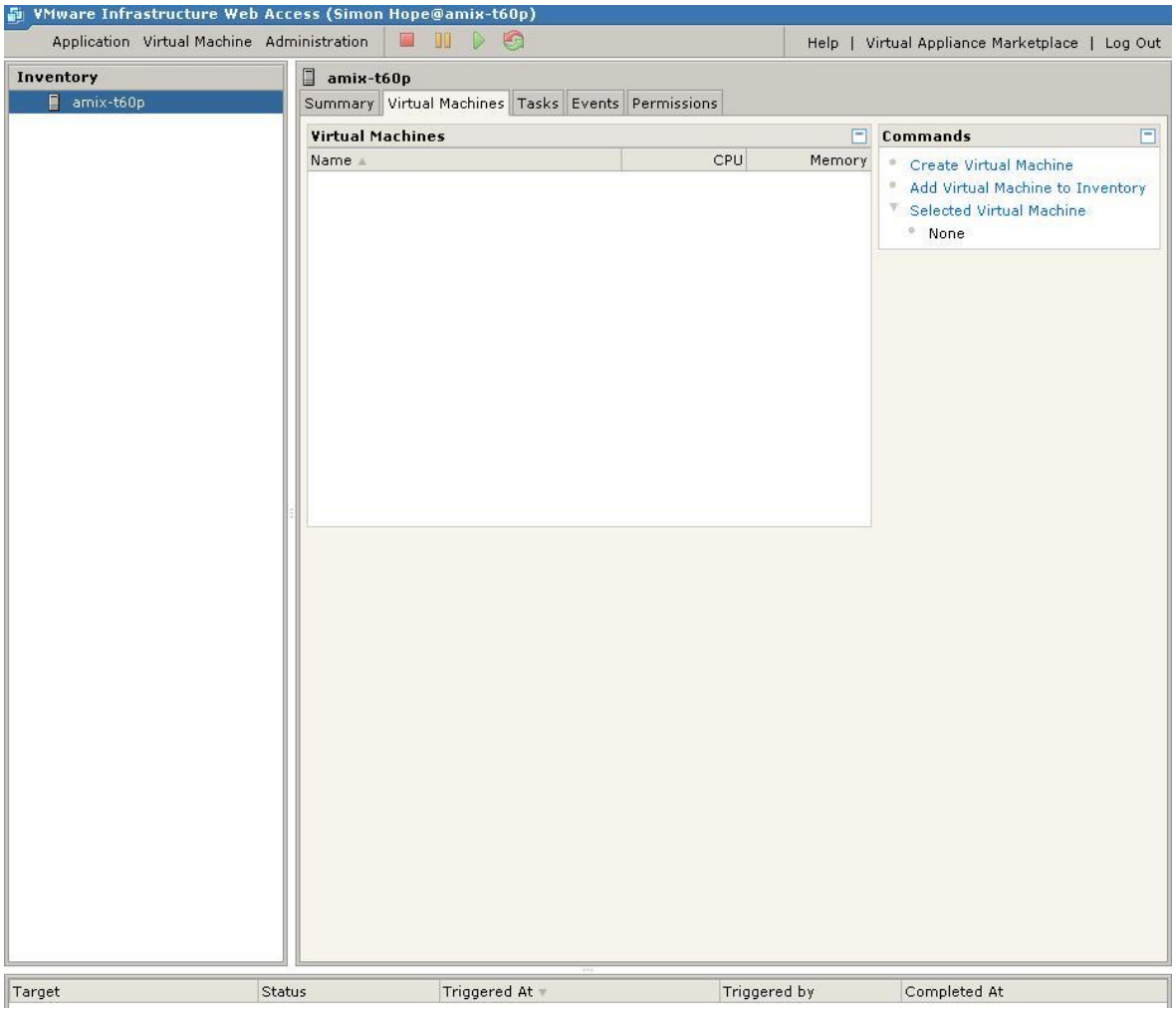
This section provides instructions for installing the Get Console Private Server on either VMWare Server 2.0 (free) (Vmx/VMDK package), or on a VMWare vSphere Cluster (OVF package). Other VMWare platforms should follow the VMWare Server instructions. Non VMWare platforms should work however are not officially supported – please see the community forum at www.get-console.com/forum for community support on non VMWare hypervisors.

## INSTALLING WITH VMWARE SERVER

To install the Get Console Private Server software in VMWare Server (version 2.0 or later):

Download the latest vmx/vmdk package from the Get Console website. Unzip into your virtual machines directory onto a datastore location of your VMWare Server.

Launch VMWare Server. Select Virtual Machines tab. Then select Add Virtual Machine to Inventory.



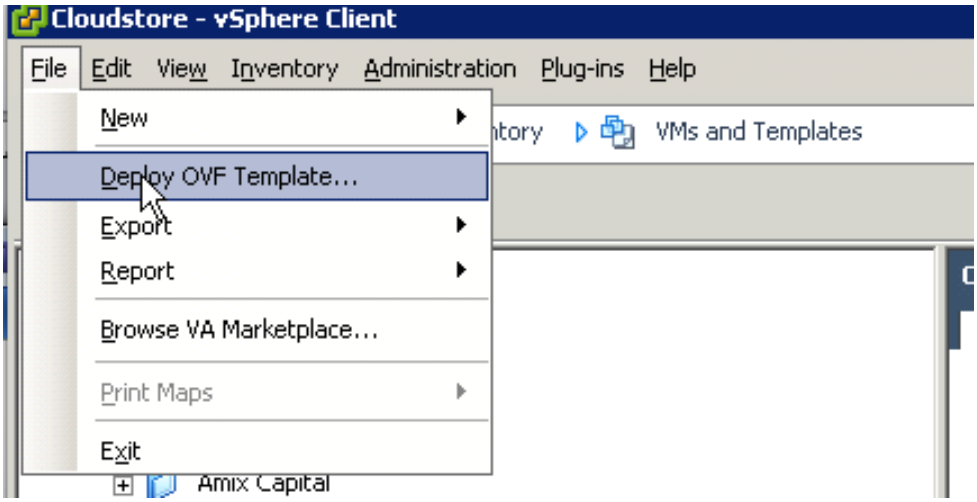

Select the .vmx file from the unzipped package from the get console web site and click open. The appliance will install.

The VM status must display a Success status at the bottom of this page to have been correctly loaded.

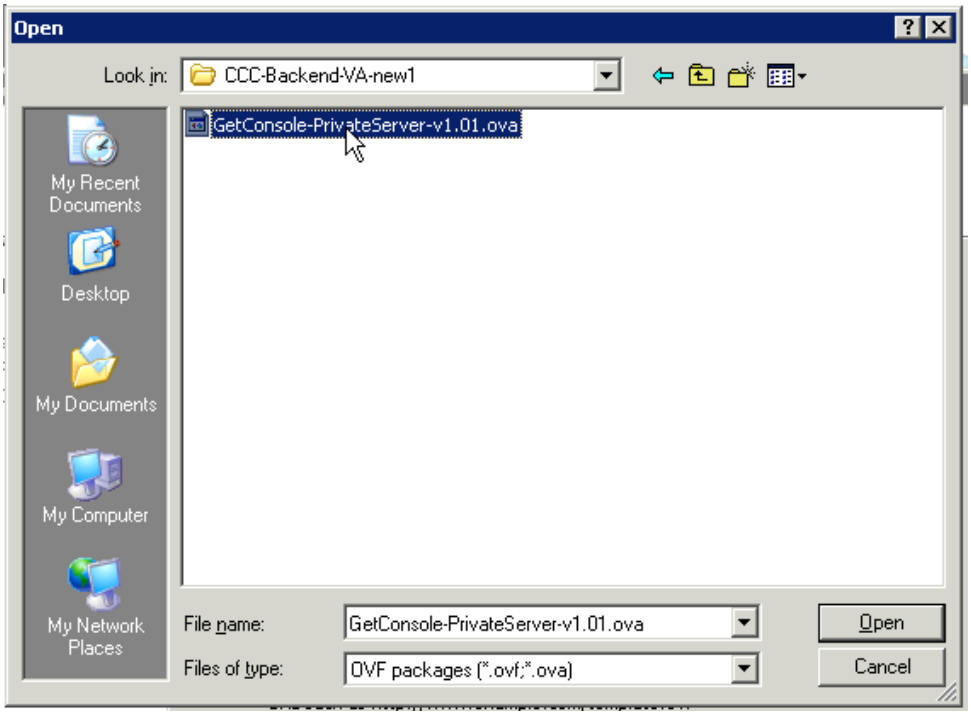
Select the play button to start the appliance. Follow the Initial Network Configuration Instructions and Web administration sections below to complete the installation.

## INSTALLING WITH VMWARE VSPHERE

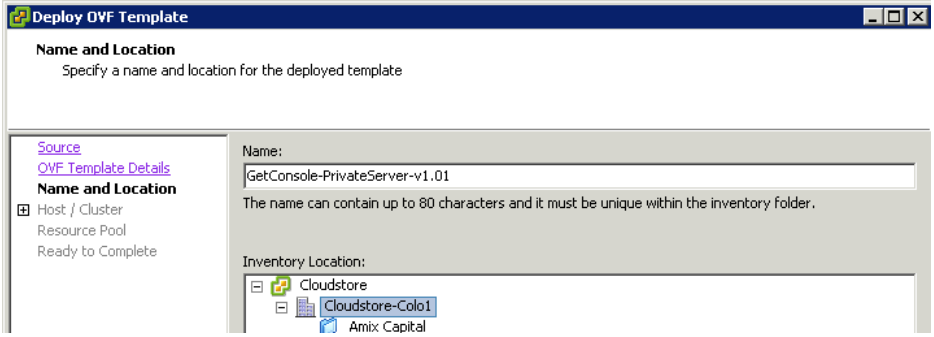
To setup the Private Server with vSphere, download the image to a datastore repository visible to the vSphere server(s). Either the VMX/VMDK or OVF package will work with vSphere. The instructions below use the OVF package.




Select the .OVA file from the downloaded package (for method to install .vmx use the New Virtual Machine wizard using the vmx/vmdk as the existing VM disk)

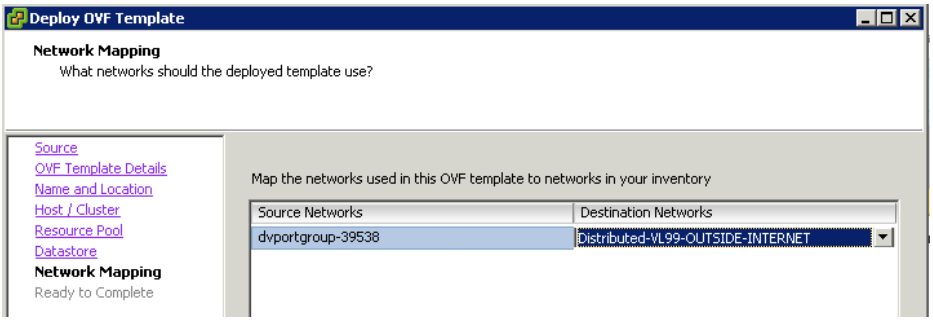



Follow “Deploy OVF Template” Wizard

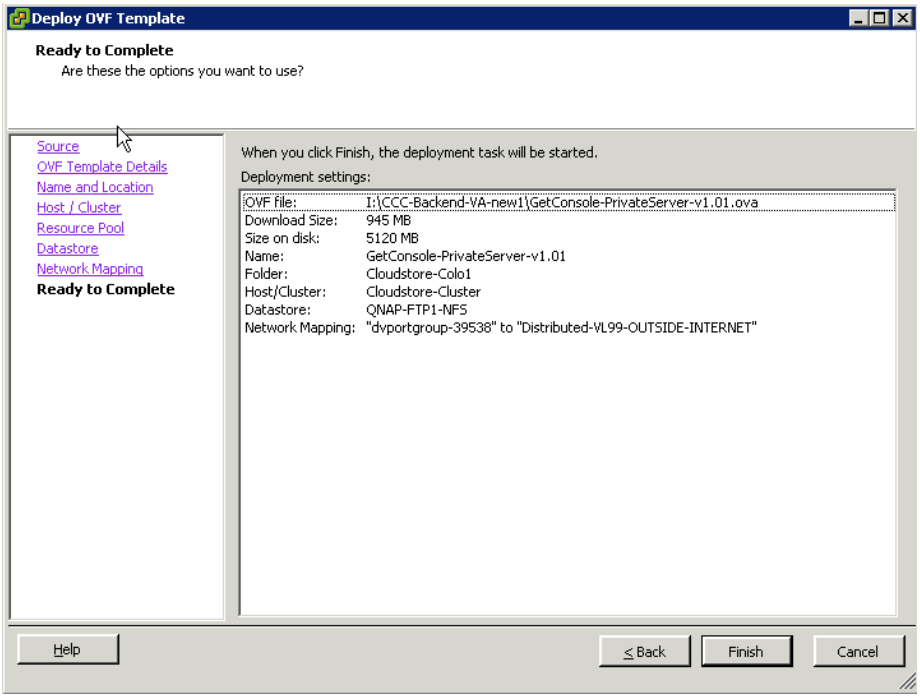



For the network settings – map the network port of the OVF template to your desired VMWare NIC or VLAN. In this example case as the appliance will have a public IP address we have mapped to an external

VLAN. If mapping to an internal or DMZ privately addressed VLAN or NIC, then for your server to be reachable from internet connected Apple iOS devices, the required NAT translations on your external firewall for TCP ports 80 and/or 443 to the Private Server will be required (see Common Deployment Architecture section).




Prior to deploying, the Wizard summarizes the options selected




Post installation, start the Virtual Appliance with the power on button, then open the web console for the virtual machine to complete the initial network configuration steps as described in the next section.

## INITIAL NETWORK CONFIGURATION

After deciding on the deployment design, the first task in configuring the Private Server is to set the IP address and default gateway. This is done by following the steps below:

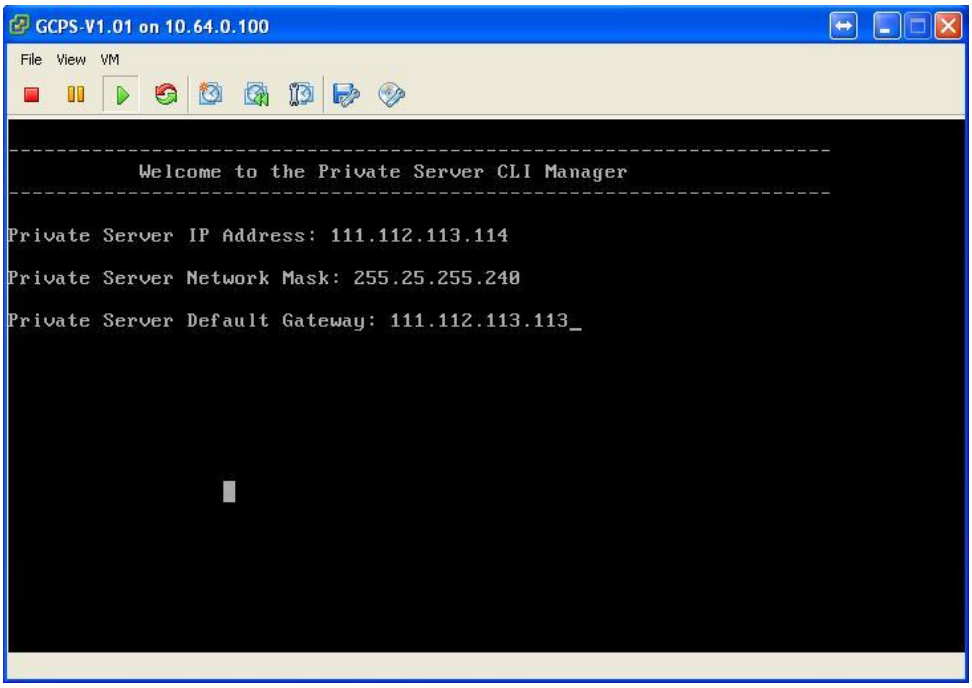
Once the Private Server is available in VMWare and has been booted, launch the Virtual machine Web Console. A Centos console will be presented with a login and password prompt.

The default username and password are

USERNAME: **webadmin**

PASSWORD: **w3badm1n!**

As the virtual appliance comes up with no network configuration, (apart from being mapped to the VLAN or Virtual NIC that was allocated during the OVF or VMX installation), this CLI wizard is used to set the initial network configuration. As DHCP is disabled, this initial network configuration must be provided via the VMWare web console with CLI interface:




NOTE: the above IP address details in the graphic are examples only. Use addressing as per your deployment design.

After completing this script, the Private Server will start with the configured IP settings. After this step all remaining configuration can be completed via the web interface by navigating to:

http://[ip-address-given-to-server]/

# PRIVATE SERVER LICENSING

## HOW LICENSING WORKS

The Get-Console Private Server is freely accessible to download from the web site, however each unique iOS device wishing to connect to the Private Server uses a Client Access License (CAL) that must be purchased in advance of use from the Get-Console.com shop.

The CAL is enforced when the Apple iOS device tries to connect to the Private Server for the first time. On first connection, the Apple iOS device will initially make a check with our license server to see if the Private Server as configured in the Apple iOS device has free licenses available, and if so will store the iOS device UDID against that Private Server and decrement the number of free licenses available. The Private Server owner can delete unwanted UDIDs consuming CAL's by contacting us at support@get-console.com (a self service web portal for this purpose will become available later in the year).

## LICENCE ACTIVATION PROCEDURE

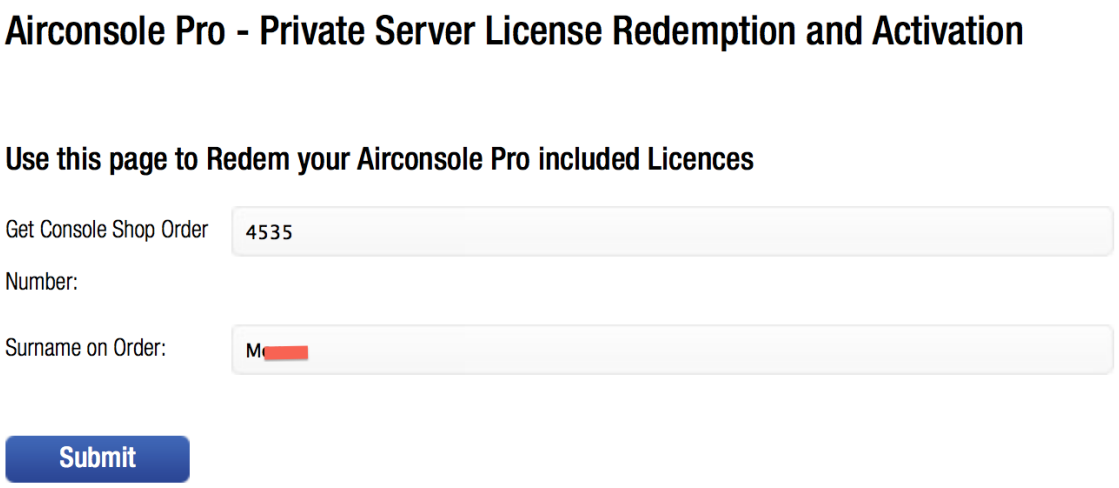
After purchasing licenses from the www.get-console.com/shop , the purchaser can obtain their license key and then apply it to their installed server.

There are 2 parts to licensing Get Console Server.

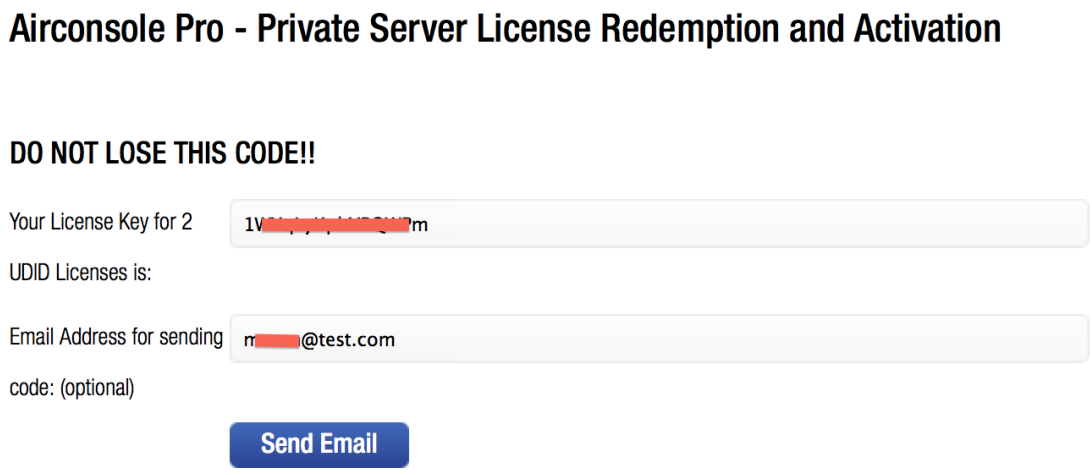
1) Obtaining License Key from www.get-console.com/redeem
2) Activating License against particular server at www.get-console.com/activation

## OBTAINING LICENSE KEYS

After purchasing Private Server licenses, or Airconsole Pro or XL products that contain bundled Private Server licenses, the Get Console website sends an email to the purchasers provided email account with their order details attached. To obtain license key go to the www.get-console.com/redeem page and enter the Get Console shop order number (not invoice number) and the surname as recorded on the email into this page.



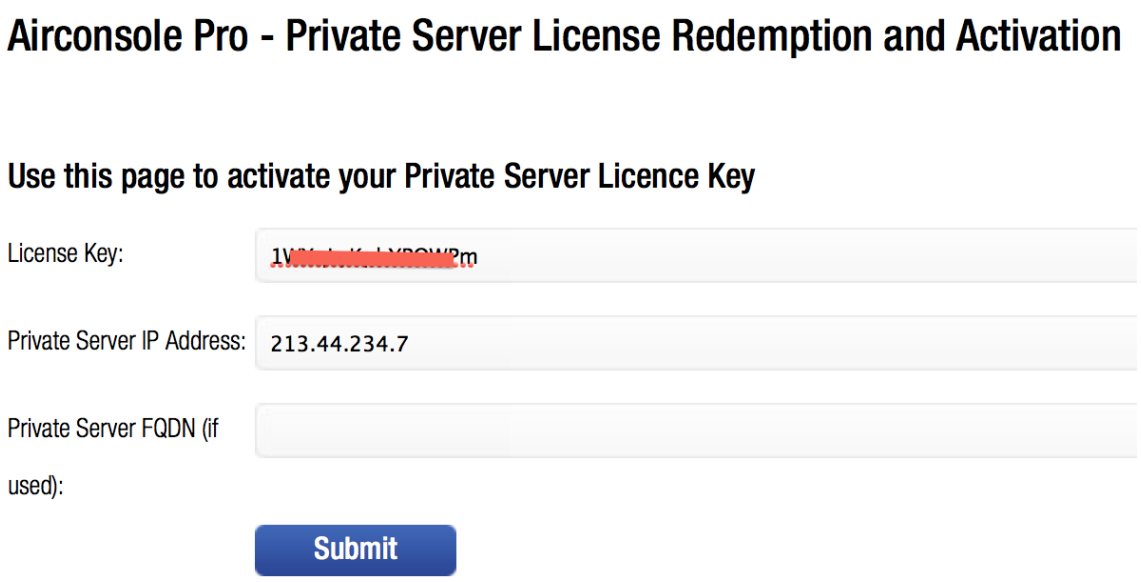

If successfully matches the order number and purchasers surname in our shop then a 15 character license key will be generated and optionally emailed to the user. An example license key is “hQiv0FTE5synSno”. The single license key contains all of UDIDs



## ACTIVATING PRIVATE SERVER LICENSE

The www.get-console.com/activation page allows for the binding of a Private Server license key to a particular Private Server.

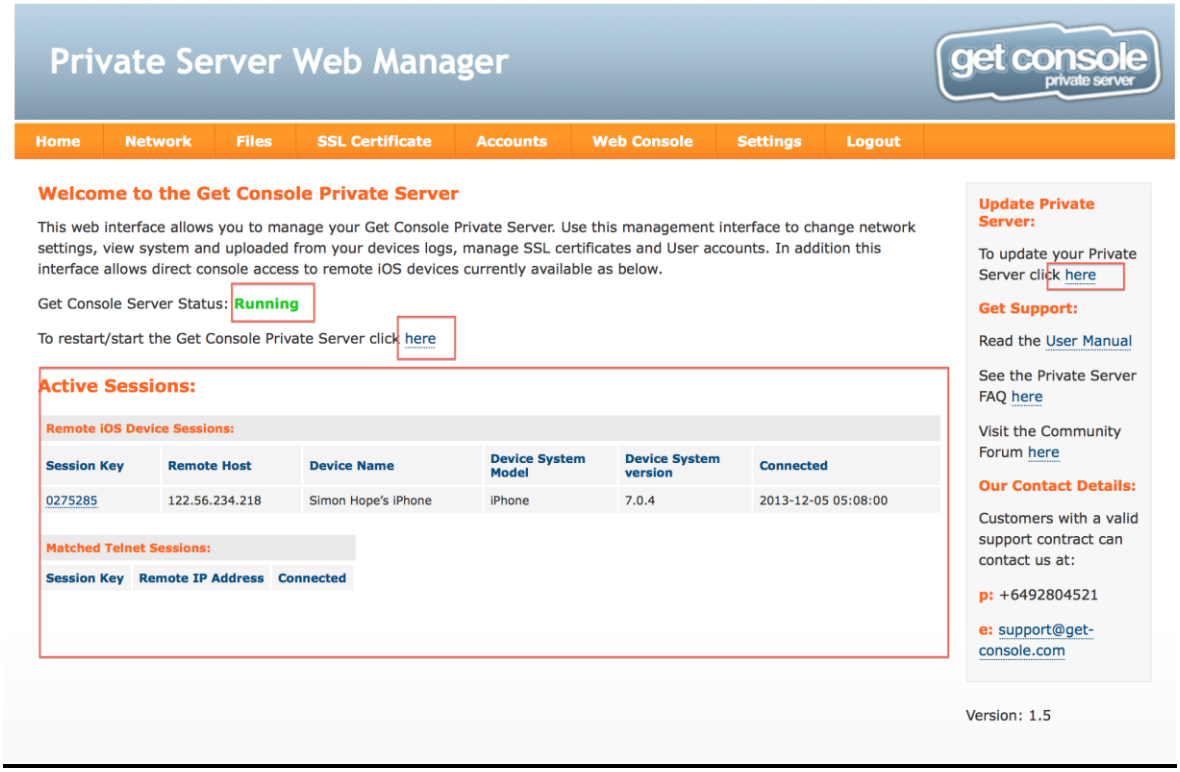
On this page enter the license key obtained from the earlier process, and the IP address and optionally the FQDN of the Private Server that the license should be applied to.




The IP address or FQDN + IP Address are used in the Get Console or (from v2.0) Airconsole Settings in order to share terminal sessions from these devices with Private Server. The first time the Get Console app attempts to share its terminal window with Private Server it communicates with our license server to validate that the IP Address or FQDN+IP Address match up with a licensed server so it is important that these values match and are correct.

# PRIVATE SERVER WEB ADMINISTRATION

## HOME PAGE




After connecting via web browser to the Private Server, and logging in using the default credentials (**webadmin / w3badm1n!)** the initial home screen above is displayed

The home page gives an overall view of server and the session status. The running status of the Get Console Private Server can be seen here as well as the incoming telnet and outgoing remote device telnet sessions. Should there be connecting to sessions select the restart button.

The active session from remote Apple iOS devices (iPad or iPhone) are listed in the Remote iOS Device Sessions table. If these iOS device sessions have been matched to a PC or Mac user connecting to the Private Server (ie through the Private Server web site, or via a telnet client) then these are listed in the Matched Telnet Sessions table.

Note to update the Private Server software to the latest version use the link in the right side bar as identified above.

## NETWORK SETTINGS

This page allows the IP address, netmask and default gateway settings to be manipulated through the web page. These are the same settings initially made via the Command Line interface.


## FILES SECTION

The main Files page provides access to the 3 types of Log files stored on Private Server, along with Generic text files, Configuration Scripts, and the ability to search within log files.


The 3 types of log files are:

1) Web Console Log Files (1)– these are web-terminal session log files generated by a web user accessing an iPad/iPhone in the field via the Private Server's Console web page. The logs are stored by session time and by the user that was logged into the shared session from the Private Server web console.

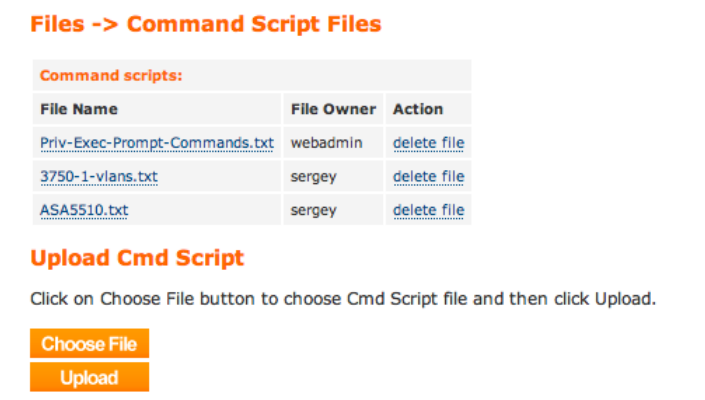

The files are owned by the Private Server user logged in and connected to the remote session. Clicking the file name link will download it.

2) iOS Device Log Files (2) – these are terminal session log files generated on iPads/iPhones in the field that can (if the user chooses to) be uploaded from the iOS device to the Private Server so that the Private Server has a centralized record of all in-the-field terminal activities.


The files are owned by the Private Server user entered on the iOS device settings at the time they were uploaded. Clicking the file name link will download it.

3) System Log files (6) – these are the log files used by the Private Server itself. For example the Tomcat logs, Apache logs and logs from upgrade process. These are generally for Get Console support to review during any system troubleshooting and are not that useful to end users.

In addition to these log files, the “Files” section allows for web users to upload text files (generally for cutting and pasting into terminal windows) or specialized configuration scripts that can be run by the Get Console app’s Scripting engine (Script Manager). Once uploaded and stored on Private Server, the iPad/iPhone users in the field can browse and download these text or .script files over-the-air (WIFI/3G) for use on field equipment.

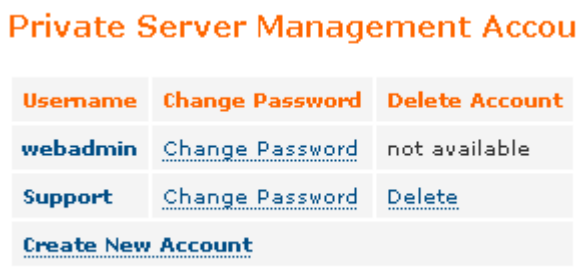


Use the Choose File and the Upload to upload config scripts/templates to the Private Server. Note that all in-the-field iOS devices will be able to see these files and download them.

## ACCOUNTS

This section of the server will allow additional user accounts to be added on the server. You can add a new username and delete usernames except the webadmin user.

Accounts are used for in-the-field iPad and iPhone users to connect to the Private Server. A valid username and password must be entered in the Get Console App settings, and will be checked when connecting to the Private Server.



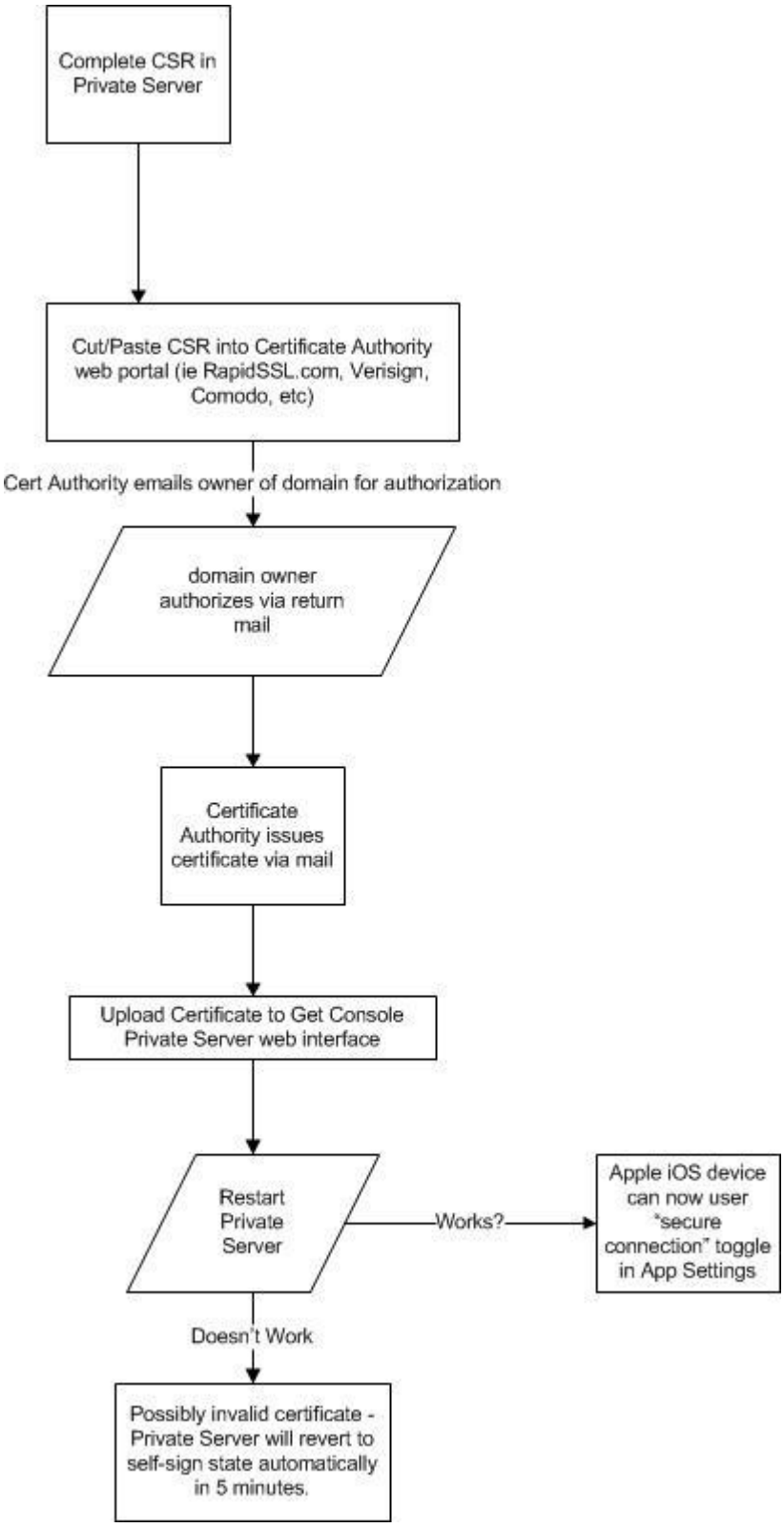

## SSL CERTIFICATE

By default the sessions between the Private Server and the remote Apple iOS device are transmitted using HTTP packets. This allows faster transfer of packets from the web interface to the remote device and back ( and therefore faster response to key strokes.)

By default the Private Server uses a self-signed certificate, however this will not allow “Secure Connection” to be enabled on the iOS device until a valid certificate has been issued by an issuing authority, and installed on the Private Server.

To enable SSL encryption between Apple iOS device and the Private Server a valid SSL certificate, issued by a Certificate Authority **trusted by Apple** must be installed on the Private Server. It is not possible to issue a Certificate from a private CA and use it on Private Server unless that private CA is trusted by all in-the-field iPads/iPhones. Generally it is much easier to buy and install on Private Server a low cost ($10) SSL Certificate that is natively trusted by iPad/iPhone.

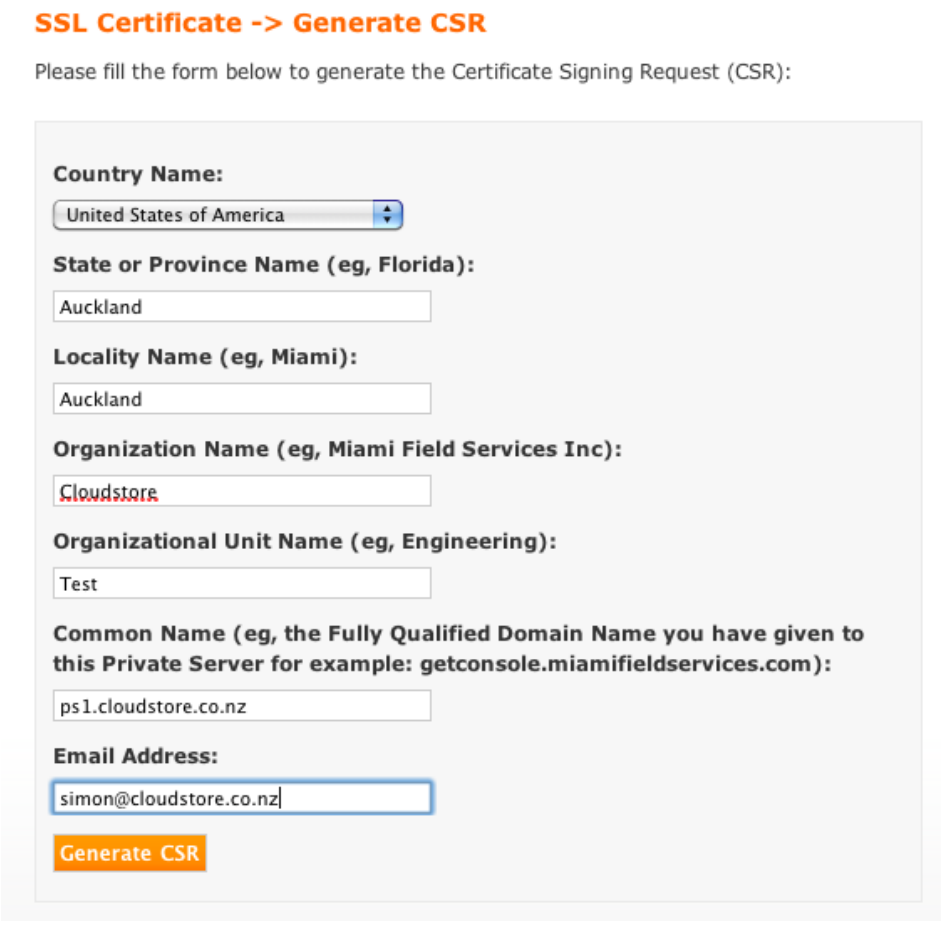
The following flowchart summarizes the process of obtaining and installing an SSL Certificate in the Private Server, and then enabling the “Secure Connection” in the iOS device App Settings. After the flow chart a detailed example of obtaining and installing an SSL certificate is covered.




## GENERATE CERTIFICATE SIGNING REQUEST

To enable SSL encryption in the Get Console Private Server the first step is to Generate a CSR (Certificate signing request)


The following form will be presented – complete this form using your own company and Common Name information :




Fill in the details of you country location, organization, name and email address. The Common Name of your organization must be a fully qualified domain name (FQDN) that you will allocate to the Private Server. This

is the most important part of the form as the certificate authority will run a query to find out who the owner is of the domain and email them to authorise the certificate request. Also the FQDN defined must be resolvable in DNS by the iOS devices.

Once this form has been filled in correctly a message will be displayed that the Certificate Signing Request has been successfully generated. Click OK


In the window that opens up the CSR will be listed. Copy and store this text to clipboard.

**Include** the ------BEGIN CERTIFICATE REQUEST------ , ------END CERTIFICATE REQUEST------ lines in the your clipboard copy

CSR:

**Use following CSR for generating SSL certificate for your Get Console Proxy Server:**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC4DCCAcgCAQAwgZoxCzAJBgNVBAYTAk5aMREwDwYDVQQIEwhBdWNrbGFuZDER
MA8GA1UEBxMIQXVja2xhbmQxFDASBgNVBAoTC0dldCBDb25zb2xlMRQwEgYDVQQL
EwtFbmdpbmVlcmluZzERMA8GA1UEAxMISm9lIFNvYXAxJjAkBgkqhkiG9w0BCQEW
F3N1cHBvcnRAZ2V0LWNvbnNvbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA8Y8UxYuPL9BsbRMH0q/W03pgPksAsGwcaB4TvVmf3FGpTE/t7T/Y
GJT6TwvSqSfy72HapB/4rg0tlhXkg6sV91knlljZJRsK4daLScnG8+NXlUlYsEzZ
Yok5eJe+7BwB4OsbS7xlfaKuFBT2ZSlFdQ8O2wrERc8dvbXcX3gvQxBkqP75LrVW
sdnBJuda63oQiikXrvNNMi9UcPWB/3y6VRTzf/qPltE2RDYpOgluum09j7SR4eZq
fqUwN9o2ZcNAQjVxWq/739e7hOpzJZsZcmuKKx3JPxjrHoeyzJlD+XvZ/R8G0F46
6uVTGIKVRXS9evxPS5YxNaSC95GztPrnKwIDAQABoAAwDQYJKoZIhvcNAQEFBQAD
ggEBABAWOJmY3qwpJ6dnkGc8opZywnatb1Tw5g9HO6eEElZFUduVjYyYj0WTjiJO
UnHV1vVFVu4tqMYjyduMSnrRNAvk1RT+HcJQFz7wRhaWHM5smBeQ4uNDppwIGaxn
/VlSzh36bkO3QcNsNzF5RDGDFTwrX4slT+4U6/+FHW2eSoH7bWQMkXfvA55sefB0
6hPZBg4jZxKbiyaZ7A1m8LFL7O5ScYFhITCyloH1Smb+dEAYjFfyEk5xVUqJzimo
FHGwxMJnceNP0LKlF41X9tH5uK9LExHchVeXqOg+GIhzPVkoVgg3IavuX9XQ8ry3
bfECiu3XAA6kmEMOx6uskF/2IgI=
-----END CERTIFICATE REQUEST-----
```

## OBTAINING SSL CERTIFICATE

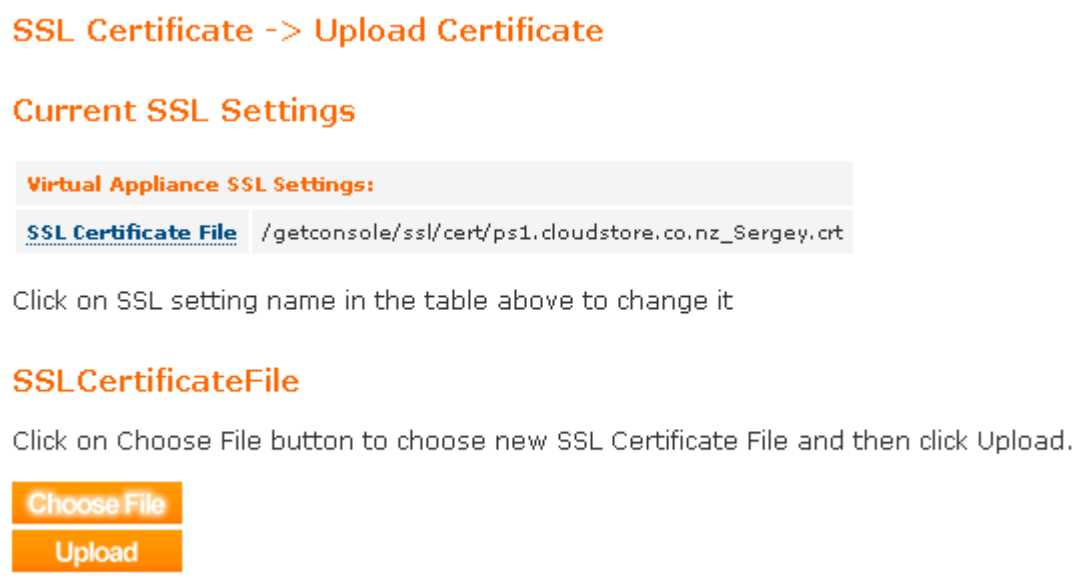
Next you will need to contact a Certificate Authority. Different Certificate Authorities have different processes for submitting CSRs, and in turn issuing the SSL Certificate. However generally the process follows as below:

Once you have paid for the certificate and submitted the CSR, the Certificate Authority organization will perform a WHOIS on the domain owner, and then email the FQDN (common name) owner for authorization to issue a certificate. Once the domain owner has mailed an approval back to the Certificate Authority (usually by clicking a link in an authorisation request email) they will send through a certificate in .crt

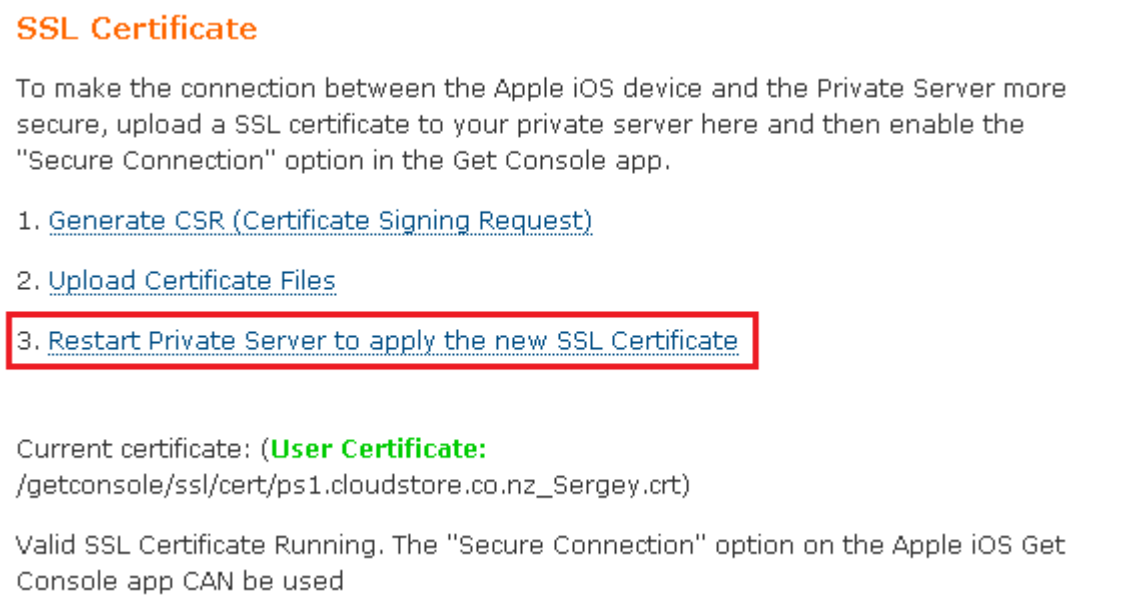
format. If the Certificate Authority offers an option as to the format of the Certificate then choose **Apache .crt format** Upload this certificate using the process as below:

## UPLOAD SSL CERTIFICATE TO PRIVATE SERVER

Using the "upload certificate file" link on the SSL Certificate page will take you to a page where you can select and upload the certificate you have been issued and upload it to the Private Server:




Once you have done this you will need to reload the server on the original SSL Certificate page. If the certificate is invalid the server will automatically revert to a self-signed certificate status within 5 minutes.




Once the SSL Certificate has been successfully installed, the SSL Page will show the green "User Certificate" as above.

The in-the-field Apple iOS devices will now be able to use the “Secure Connection” setting. If this setting is selected while a self signed certificate is still installed on the Private Server an error about invalid Private server will appear.


## UPDATING THE PRIVATE SERVER SOFTWARE

Starting from Private Server version 1.2, the Virtual Appliance and Database files can be updated without re-installing the Virtual Appliance. This feature will be used to non-distruptively update Private Servers from version 1.2 to version 1.3 and later.

There are 2 methods to update the Private Server software

1) Semi-Automatic Updates
2) Manual Updates

Although the Get Console developers test all Private Server updates, There is currently NO option to rollback an update after it has been installed. Because of this we recommend using the VMWare or “Snapshot” facility to take a Snapshot of the Virtual Appliance before applying the update. Should an update cause corruption to the Private Server, revert to that VMWare snapshot and contact Get-Console support.

## SOFTWARE UPDATES

There are 3 options on the Software upgrade page.

**Update Options:**

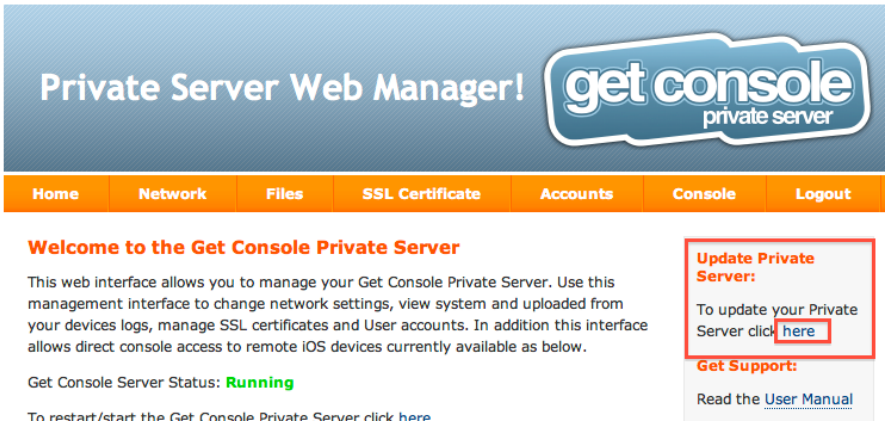
1. Update your Private Server automatically (Internet connection required)
2. Update your Private Server manualy
3. Update web server to the latest version (Internet connection required)

1) Upgrades between a point release can generally be performed automatically for example an upgrade from version 1.5.1 to version 1.5.2
2) Upgrades between major releases (1.5.1->2.0.0) and **some** minor releases (1.5.1 -> 1.6.0) can only be performed via the manual method. This will be noted on the www.get-console.com/private-server page.
3) Upgrades to the underlying Apache server can be performed automatically and independently of the Private Server. We recommend checking and patching the webserver regularly to keep web security vulnerabilities minimized.

## AUTOMATIC UPGRADES

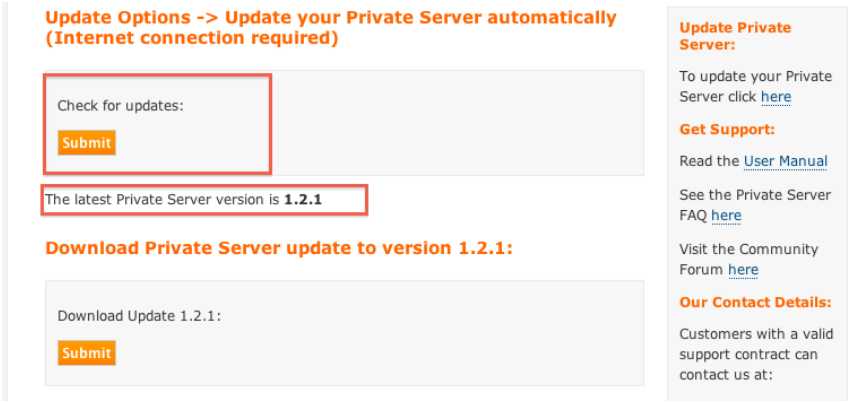
The Semi-Automatic update process involves checking the Get-Console.com website for new Private Server sub versions for the Major.minor release currently installed, if a new version exists downloading it and then if downloaded successfully, installing it. No restart of the Private Server is generally required.

To check for new versions of Private Server click the “Check for Updates” button on the home page (or any of the other Private Server pages) located on right hand side bar

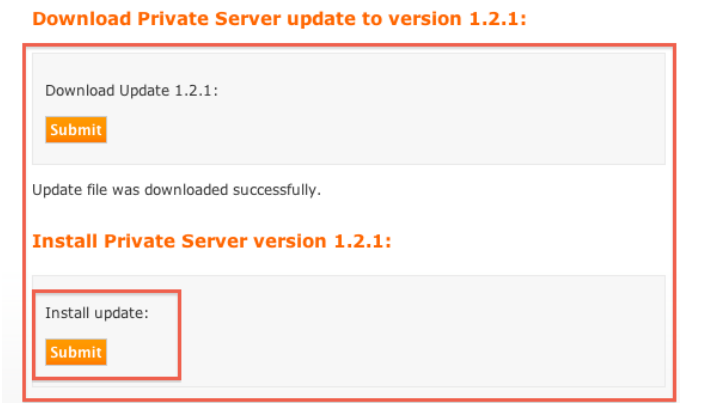



Select option 1: Automatic Updates (Requires Internet Connectivity)

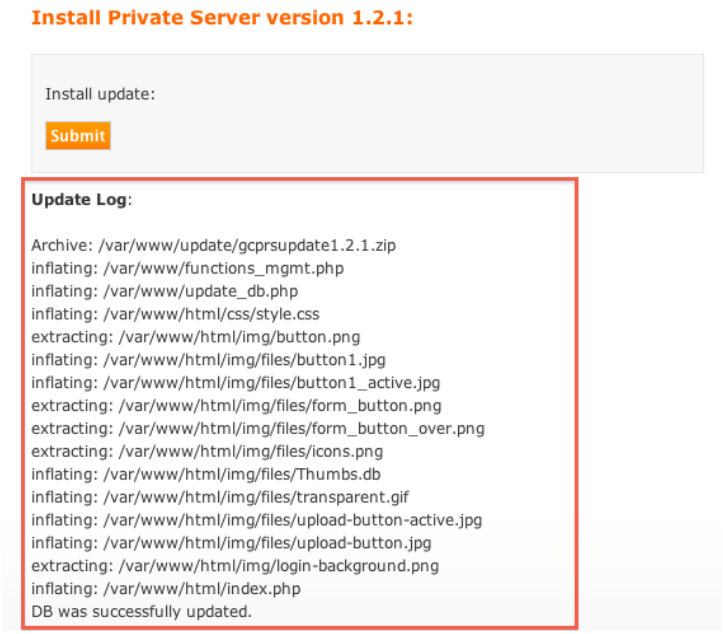

If a new update is available then it will be presented as available to download – in the case below version 1.2.0 can be upgraded to 1.2.1 is available:




After downloading, the dialog box will allow for installing



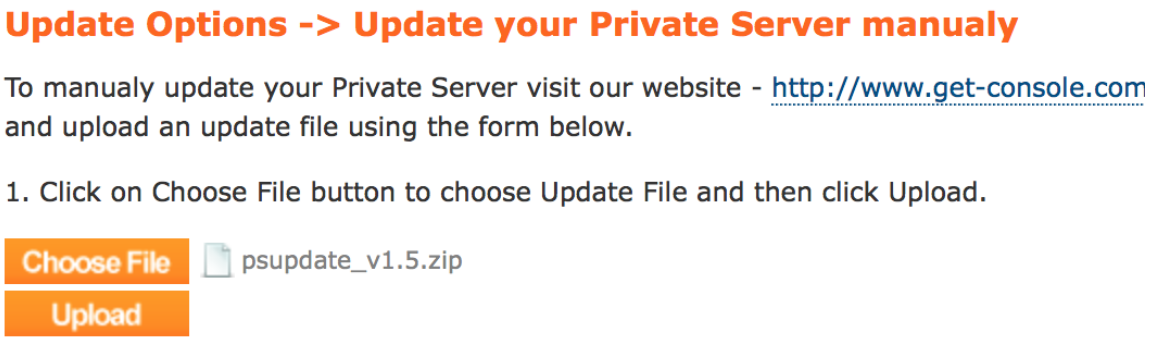

Clicking on “Submit” button under Install Update will install the downloaded patch file. The patch file will unpack and install the changes to the Virtual Appliance. The last line should say “DB successfully updated”.




## MANUAL UPDATES

The Manual Update process requires the download of the update package from the get-console.com/private-server webpage, and then uploading this package to the Private Server.

Generally the Manual Update method will be needed when many O/S level files need to be patched or added. This means that the server will be rebooted during the upgrade process.




After uploading, click Submit button under the "Install update" heading. Note the checkbox to perform the install unattended. Clicking submit button will reboot the server, and during the reboot the server will unpack the update zip file and run the associated install scripts. This process can be viewed via the VMWare console if

If the unattended install check box is NOT ticked, then the update script will prompt user for confirmation of the script to run and timing of the reboot via the VMWare console terminal. The terminal needs to be accessed within 30 seconds of pressing submit or the upgrade will be cancelled and the original version of the Private Server will boot.

## CONFIGURING IOS DEVICE GET CONSOLE APP TO USE PRIVATE SERVER

To enable a particular Apple iOS device to use the private server, 4 fields must be populated correctly in the Get Console app Settings:

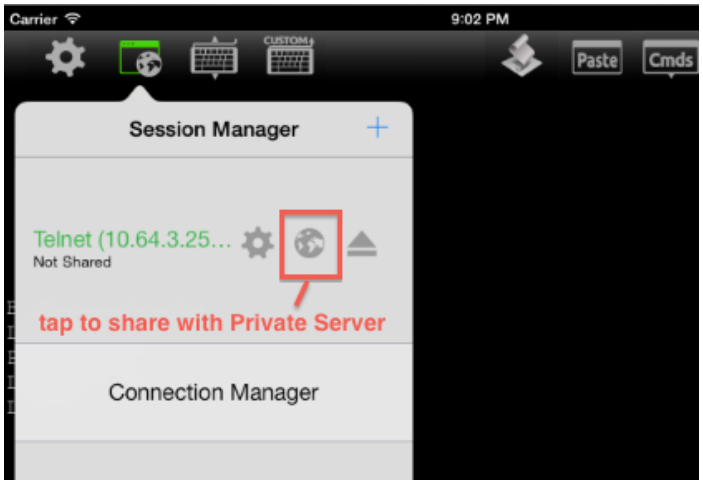
1) the IP address or FQDN details of the Get Console Private Server. An FQDN is needed to support the Secure Connection option. These details **MUST** match the details in the license activation process described in above section.
2) a valid username for a user defined on the Private Server must be entered into username field (for example "**webadmin**"
3) the password for that Private Server hosted username must be entered correctly (for example "**w3badm1n**!"
4) the Remote Server setting must have "Private Server" selected (as opposed to North America, Asia Pac or Europe)

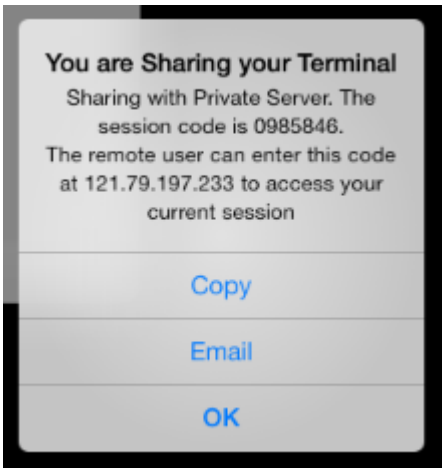
Please note that ALL fields are **case sensitive**

Do NOT enable the "Secure Connection" switch in the App until a valid SSL Certificate has been installed on the Private Server. See the SSL Certificate Section below.

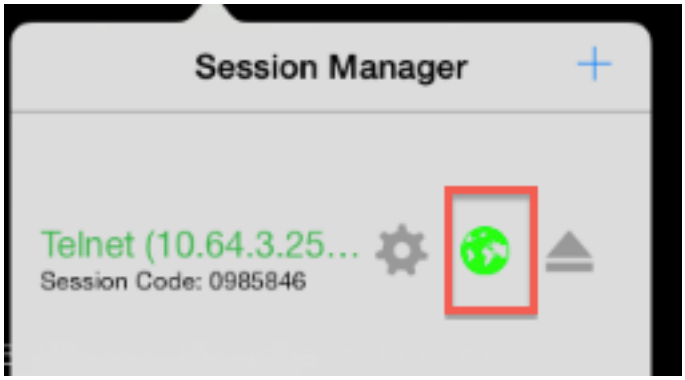
An example of valid iOS device settings is below:


Once these settings have been configured, return to the main terminal window in the App, and press the Connect Session button (top nav bar in Terminal window, second from left button), and then select “Share Session”

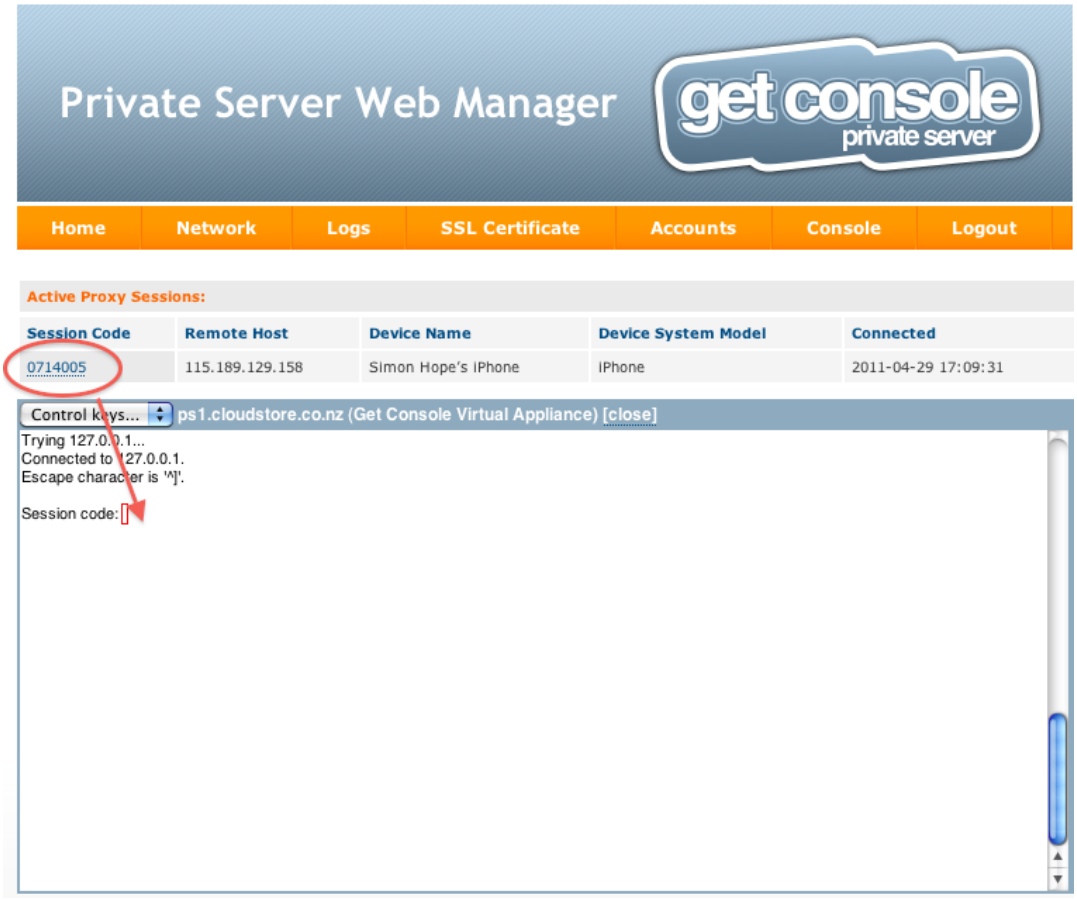



Once the session is shared, a pop-up appears in the iOS device provides the allocated session code. Session codes to Private Servers always start with “0” The Globe icon will be green when session is being shared:



The remote PC user can now see the remote iOS device in the Private Server home page, and also in the Console page.




The PC user can also use a generic telnet client to access to remote iOS device terminal session using port 2323.

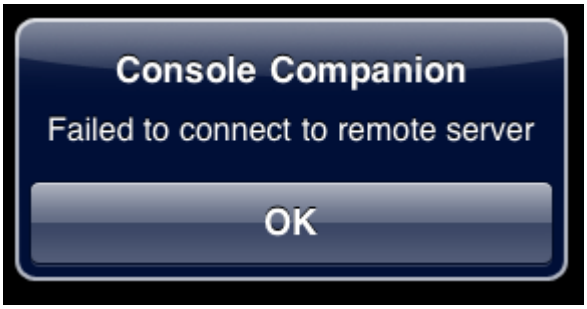
To use a third party telnet client rather than the web client, simply telnet to the Private Servers IP address (or domain name) on TCP port 2323. A session code prompt will be presented where the PC user can enter the code of the remote iOS device to be connected.

The Console page will allow the PC based user to access the console session of the remote iOS device.

Once you select this page you will be prompted for a session code, however simply clicking on one of the available session codes displayed above the console window will automatically enter the code and connect to the remote iOS device session.

# TROUBLESHOOTING CONNECTIVITY TO PRIVATE SERVER

## GENERAL CONNECTIVITY ISSUES

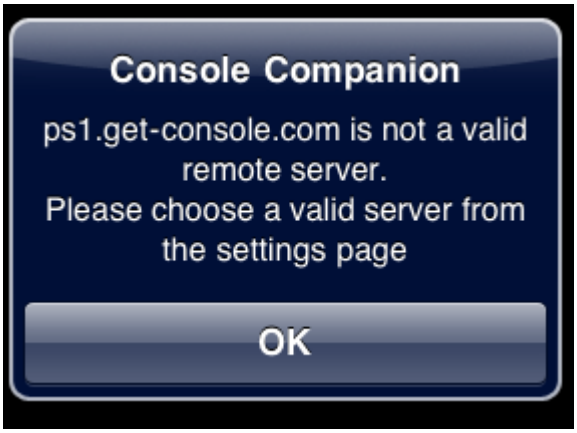



The above message will be displayed on the apple iOS device when:

1) There is no connection to the internet or private network where the Private Server resides; or
2) The FQDN of the Private Server (if configured as FQDN rather than IP address) cannot resolve to an IP address via the iOS device; or
3) The Private Server is nor reachable (switched off, not routable or possibly firewalled on ports 80 or 443)
4) **Where "Secure Connection" is selected in the Get Console App, but no valid SSL Certificate has been installed on the Private Server**

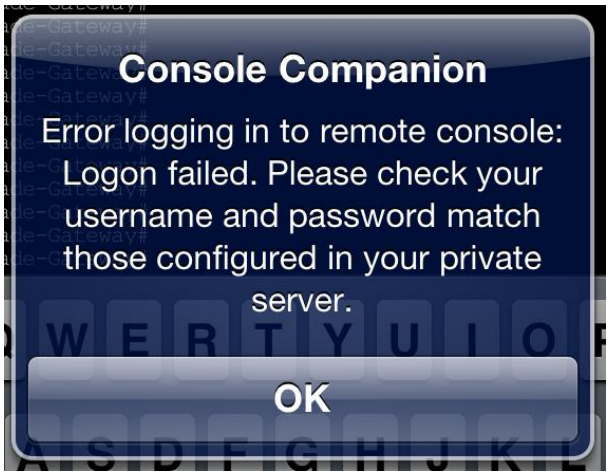
Please correct the connectivity issues for the iOS device or Private server, or disable "Secure Connection" in settings then try again.

## SERVER NOT RECOGNIZED BY LICENSE SERVER




The above message will be displayed on the Apple iOS device when although there is internet connectivity for the iOS device, the Private Server IP address or Hostname has not yet been enabled on our license server. Please purchase a license from the www.get-console.com/shop or if one has been purchased already please provide the server details to activations@get-console.com to ensure it has been activated.

## INCORRECT USERNAME OR PASSWORD




This error occurs when username has either not been defined on Private Server (Accounts tab), or has been defined but the password is wrong. Note that both Username and Password are case sensitive.

## LICENSE ISSUES

Where the Private Server is defined on our License Server, but does not have any available licenses then when connecting the user will receive an error like below.


The possible error codes (useful for Get Console Support) are:

0001 = Private Server Defined but no License Assigned

0002 = Private Server Defined, License Assigned but no un-expired licenses available

0003 = Private Server Defined, License Assigned but all existing licenses are used up by other devices

Other error codes maybe added in the future. In all these cases if you have purchased a Private Server license from the Get Console shop and requested its activation/assignment but are still receiving this error then please contact Get Console support via email at support@get-console.com

When using the www.get-console.com/activation method to load licenses onto Private Servers, the process takes around 2 minutes. For manually activated licenses there is a lead time of 4 hours from purchase for our staff to upload the CAL license details to the license server.